

UNITED STATES DISTRICT COURT

for the
Eastern District of North Carolina

FILED

JUL 13 2023

PETER A. MOORE, JR., CLERK
US DISTRICT COURT, EDNC
BY BG DEP CLK

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)TCL BRAND PHONE, IMEI: 01569500861147, TCL BRAND PHONE,
IMEI: 016144002543799, SAMSUNG BRAND PHONE, IMEI:
350593473858405, AND ONE SAN DISK BRAND, 32GB THUMB
DRIVE

Case No.

5:23-mj-1792-RJ

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

TCL BRAND PHONE, IMEI: 01569500861147, TCL BRAND PHONE, IMEI: 016144002543799, SAMSUNG BRAND PHONE, IMEI: 350593473858405, AND ONE SAN DISK BRAND, 32GB THUMB DRIVE as described in Attachment A.

located in the Eastern District of North Carolina, there is now concealed (identify the person or describe the property to be seized):

See Attachment B hereto and incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2251	Sexual Exploitation of a Minor
18 U.S.C. § 2252A	Receipt, and/or Possession Child Pornography, and/or Access with Intent to View

The application is based on these facts:
See attached affidavit which is attached hereto and incorporated herein by reference☒ Continued on the attached sheet.☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.Erika M. Rodriguez
Applicant's signatureErika Rodriguez, SA Army CID
Printed name and titleOn this day, Erika Rodriguez
appeared before me via reliable electronic means, was
placed under oath, and attested to the contents of this
Application for a Search Warrant.Date: July 13 2023Robert B. Jones, Jr.
Judge's signature

City and state: Wilmington, North Carolina

Robert B. Jones, Jr., United States Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NORTH CAROLINA
WESTERN DIVISION
5:23-CR-200-M

IN THE MATTER OF THE SEARCH OF)
INFORMATION ASSOCIATED WITH)
TCL BRAND PHONE, IMEI:)
01569500861147, TCL BRAND PHONE,) **FILED UNDER SEAL**
IMEI: 016144002543799, SAMSUNG BRAND)
PHONE, IMEI: 350593473858405, AND ONE) Case No.
SAN DISK BRAND, 32GB THUMB DRIVE)

AFFIDAVIT IN SUPPORT OF APPLICATION

I, Erika Rodriguez, being duly sworn, depose and state that:

INTRODUCTION

1. I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I am a Special Agent with the Department of the Army Criminal Investigations Division (CID), and am currently assigned to the Carolinas Field Office, Fort Liberty, NC. I have been employed by CID since 2016. My duties include investigations of violations of the Uniform Code of Military Justice, as well as federal criminal law in connection with crimes committed on Fort Liberty, NC, (formerly known as Fort Bragg) which is federal exclusive jurisdiction. I have approximately seven years of experience investigating violations of the Uniform Code of Military Justice and federal law, to include violent criminal cases such as homicides, kidnapping, rape, acts of terrorism, and crimes against children. Through formal and on the job training, I have developed experience in investigations dealing with violent offenses as set forth in the United States Code. In the course of

these investigations, I have requested digital information in connection to Child Sexual Abuse Material (CSAM) and reviewed and analyzed the returned information in a multitude of cases. As a CID Special Agent, I am authorized to investigate violations of federal law and to execute warrants issued under the authority of the United States. This investigation is being conducted jointly with the Fayetteville Resident Agency, Federal Bureau of Investigation.

PURPOSE OF AFFIDAVIT

2. I make this affidavit in support of an application for a search warrant for the search of digital devices seized pursuant an inventory of personal property and due to exigent circumstances from Barracks Room 201B, 4822 Gruber Road, Fort Liberty, NC 28310, for evidence pertaining to Child Sexual Abuse Material. The devices include one TCL brand phone, IMEI: 01569500861147, one TCL brand phone, IMEI: 016144002543799, one Samsung brand phone, IMEI: 350593473858405, and one San Disk brand, 32GB thumb drive, which are currently maintained within law enforcement custody. The property to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2251(A) (production of Child Sexual Abuse Material (CSAM)), 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) (receipt of CSAM, and attempt) and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of, or access with intent to view, CSAM, and attempt). Upon receipt of the information described in Attachment B, government-authorized persons will review that information to locate the items described.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that the violation of 18 U.S.C. §§ 2251(A) (production of Child Sexual Abuse Material (CSAM)), 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) (receipt of CSAM, and attempt) and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of, or access with intent to view, CSAM, and attempt), was committed within the special territorial or maritime jurisdiction of the United States, was committed by Jason C. MANUELITO Jr. while located on Fort Liberty, North Carolina. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is a “court of competent jurisdiction” as defined in 18 U.S.C. § 2711. *See* 18 U.S.C. §§ 2703(c)(1)(A). Specifically, the Court I “a district court of the United States (including a magistrate judge of such court) . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. On or about July 2021, the Carolinas Field Office (CFO), CID, was notified by NCMEC, that Army Specialist JASON C. MANUELITO Jr. uploaded images depicting CSAM to Kik Messenger in May 2021. MANUELITO was certified by the Army as a Military Occupational Specialty “25B” defined as an Information Technology Specialist. The Army states the following job information on their public access website “As an Information Technology Specialist, you’ll maintain, process, and troubleshoot military computer systems and operations. You’ll deal with highly sensitive information and need to have technical skills and aptitude for programming and

computer languages.” MANUELITO is certified in CompTIA Fundamentals, is a certified Fiber Optics Installer, and obtained a 3M certification through the US Army.

7. A review of the NCMEC report revealed Kik, Inc./Media Lab reported an incident of CSAM in connection with the Kik account "https://kik.com/blossomgirlgabby16_jr2". The subscriber information was documented as Gabriela Garcia, "gabsgarcia2203@gmail.com", username: "blossomgirlgabby16". Subscriber activity showed user account was created 28 Mar 21, registration email of gabsgarcia2203@gmail. Further, the subscriber activity revealed 3 images were uploaded in a messenger platform to another user or group, utilizing IP Address 65.191.89.74, 5/12/2021 4:50:08 AM.

8. North Carolina (NC) State Bureau of Investigation (SBI) Administration Subpoena: A review of the subpoena revealed a request for Charter Communications Legal Department for the IP Address 65.191.89.74, 5/12/2021 4:50:08 AM.

9. Charter Communications Subpoena Results: A review of the results revealed subscriber information pertaining to IP Address 65.191.89.74, 5/12/2021 4:50:08 AM, belonged to SPC MANUELITO, with the military address of Barracks Room 201B, 4822 Gruber Road, Fort Liberty, NC 28310.

10. On or about 3 September 2021, CID received three Cyber Tips from NCMEC indicating MANUELITO uploaded images depicting child pornography using Google and Drop Box. A review of Cyber Tip 94257673, revealed about 0117, 2 Jul 21, an IP address identified by Charter Communication as belonging to MANUELITO was used to upload six images of child pornography using Drop Box. Drop Box listed the user as "Jared Manuel" using email address "jaredmanuel35@gmail.com". A review of Cyber Tip 94257859, revealed about 0122, 2 Jul 21,

an IP address identified by Charter Communication as belonging to MANUELITO was used to upload five images of child pornography using Drop Box. Again, Drop Box reported this account belonged to "Jare Manuel" using email address "jaredmanuel35@gmail.com". A review of Cyber Tip 94279579, revealed about 0837, 2 Jul 21, an IP address identified by Charter Communication as belonging to MANUELITO was used to store four images of child pornography using the Google Photos infrastructure.

11. A Regional Organized Crime Information Center Search (ROCIC) was conducted for jasonmanuelito97@gmail.com and gabsgarcia2203@gmail.com and found that they had a common association with Instagram accounts; @babsi_gmail belonging to Barbara Gelinska and @Shashik5614gmail.com5 belonging to "Shashi". These common associations suggest Gabriela Garcia was a pseudo name for MANUELITO.

12. In September 2021, MANUELITO was advised of his legal rights, which he waived and provided a statement. MANUELITO stated from approximately November 2019 to June 2020, he engaged in an online relationship with a juvenile female who called herself "Jackie". MANUELITO stated they met on Instagram where he sent her sexually explicit photos, and received CSAM from her on Snapchat, a social media platform. MANUELITO stated he saved the CSAM of "Jackie" on his Samsung Galaxy cellular phone. Additionally, he admitted he saved CSAM in his Dropbox in a folder labeled Jackie. MANUELITO admitted he knew Jackie was 16 years of age and knew what he was doing was illegal. MANUELITO further admitted from approximately January to July 2020, he solicited an additional juvenile female, "Lolaka", who he believed resided in Salt Lake City, UT. MANUELITO admitted he sent her sexually explicit photos, and received CSAM from her. MANUELITO further stated he discussed traveling to Salt

Lake City, UT to meet the juvenile victim. MANUELITO admitted he knew Lolaka was 16 years of age and knew what he was doing was illegal. MANUELITO denied he was still in contact with the Lolaka or Jackie. MANUELITO further admitted he was involved in a Discord social media platform group with two females, ages 13 and 16. He stated they would refer to him as “dad” and he would refer to them as his “daughters”. He stated they would only send him images of themselves that were fully clothed. MANUELITO stated he previously solicited free sexually explicit material on Kik Messenger groups. MANUELITO stated he received both adult sexually explicit material, and CSAM. He stated he would obtain several folders with thousands of files of unknown sexually explicit material and save it into his Google Dropbox account. He subsequently shared the links in group chats in Kik Messenger. MANUELITO further admitted the account associated with gabriellagarcia2203@gmail.com, which appeared to be operated by a juvenile female, was in fact his account. MANUELITO admitted he used a fake Kik account where he posed as a juvenile female to more easily obtain content.

13. On or about September 2021, SA Vazquez obtained a Military Magistrate Authorization, authorizing CID to conduct a search and seizure of all electronic devices found in MANUELITO’S barracks room, and his person for evidence of CSAM. Pursuant to the authorization, a search was conducted and approximately thirteen items of evidence were seized.

14. In November 2021, SA Vazquez obtained a Military Magistrate Authorization, to conduct further Digital Forensic Examination of the electronic devices seized.

15. In June 2022, CID received and reviewed the Digital Forensic Examination report of MANUELITO’S digital devices, which revealed evidence of receipt, possession and production of CSAM. The examination revealed MANUELITO’S Samsung Galaxy smartphone was

associated with the following information: phone number 928-679-5695, various social media platforms, to include those described by MANUELITO during his interview. During the review of the digital evidence seized it was determined MANUELITO was in direct communication with children, wherein he engaged in sexually explicit communication. Digital media was located that documented MANUELITO both instructed, shared, and received CSAM material from female children. This data included but was not limited to, picture-in-picture (PIP) videos, wherein MANUELITO engaged in a video chat with a child, and both he and the child are simultaneously visible on the screen of the recording. MANUELITO and the child are depicted masturbating.

16. On or about 20 Sep 22, Lahna Copeland (LAHNA), date of birth (DOB) August 27, 2006, was interviewed at the Fayetteville Resident Agency FBI Office, 3401 Village Drive, Suite 200, Fayetteville, North Carolina (NC) 28304. The forensic interview was conducted by Jodie Hively, Child/Adult Forensic Interview Specialist. LAHNA was identified from Instagram account association and CSAM located on MANUELITO'S devices. Instagram is a photo and video sharing social networking service owned by American company Meta Platforms. Upon interview LAHNA reported she was a victim of online child exploitation. LAHNA reported she agreed to provide CSAM of herself online, in exchange for payment. LAHNA lived in a modular trailer home at the time of the interview. LAHNA stated she was not aware of anyone by the name of Jason MANUELITO and did not identify his image.

17. Additionally, screen recordings were recovered on MANUELITO'S ASUS computer, that depicted MANUELITO sent two Cash App payments on between October 2019, and January 2020. The payments were sent through Instagram messenger to an account with the username "babxi.mya". Cash App is a mobile payment service available in the United States and

the United Kingdom that allows users to transfer money to one another and can interface with other applications such as Instagram. The Instagram account was identified as belonging to Miss MAYA Benale, a 16-year-old female. According to screen recordings saved on MANUELITO'S ASUS computer, within minutes of the money transfer he received CSAM pictures and videos of MAYA.

18. Subpoena returns from Cash App documented the same date, amount, and description of payments were associated with the account name "Sapphire2015." Cash App subpoena returns further documented "Sapphire2015" utilized bank account number 4744880050038783 as their form of payment to MAYA. Similarly, display name "Shadows" utilized the same card number when paying Benale. Bank of America subpoena returns, documented account number 4744880050038783 belonged to MANUELITO.

19. MANUELITO'S digital devices further documented association with multiple Instagram accounts that appeared to be owned and operated by him. MANUELITO'S Samsung S7 cellular phone, contained screen recorded videos that depicted the user of the device, assumably MANUELITO, actively operating the accounts "jasminerose_1622", "royal_blue7000", "sapphire_420", and "starlite_sapphire". Videos depict the user receiving suspected CSAM via Instagram and saving the videos through the screen record function on the phone, which in-turn displays the application and usernames.

20. Subpoena returns for the Instagram accounts associated with usernames "jasminerose 1622", "royal_blue7000", "sapphire_420", and "starlite_sapphire", documented IP addresses that were all associated with Ft. Liberty, NC. The accounts for usernames "jasminerose 1622" and "sapphire_420" were further shown to be in use in July 2021. In October

2022, an additional subpoena was served which documented the account “jasminerose_1622” was still in use, with a last login date of September 2022.

21. The LA/Sacramento FBI office, is investigating a separate child exploitation case, wherein MANUELITO appeared to be a repeat purchaser of CSAM from their subject, BARRIOS. The information was documented through Instagram communication between BARRIOS and the Instagram account username “tyredye__”. An account later determined to be verified through the phone number belonging to MANUELITO. MANUELITO sent money to Cash App account “\$lafamosajoceyy” and labeled the payment “groceries”. In the conversation their subject calls MANUELITO a loyal customer from previous exchanges. During the conversation their subject asks MANUELITO “What happened to everything u have bought?” MANUELITO responds “Miss girl, I broke my old phone and I didn’t save it to a Dropbox”, wherein BARRIOS stated “So u lost everything from the past yrs?”. This communication occurred in January 2022.

22. Subpoena returns for Instagram accounts associated with phone number 928-637-4811, documented the account associated with usernames “tyredye ”, “sapphire__420”, “royal_blue7000”, “starlite_sapphire”, and additional usernames, was closed on 30 September 2022.

23. On or about 10 September 2021, MANUELITO was given a written and lawful military order from his Commanding Officer to not possess digital devices including but not limited to smart phones, tablets, and computers capable of having an internet connection, with the exception of gaming consoles not to be used on the internet. This order was re-affirmed through a written army counseling statement dated 7 November 2022, signed by MANUELITO on 8

November 2022. Violation of this order would constitute as a violation of military law under Article 92 of the Uniform Code of Military Justice, for Failure to Obey a Lawful Order.

24. Additional subpoena returns dated 29 November 2022, for Instagram accounts associated with phone number 928-637-4811, documented the account associated with the username “technerdd42” was last logged in on 13 November 2022. The return documented the account name was changed approximately 15 times, with a recent names of “ghostmemories2023”, and “unknowndestination2023”. In my training and experience frequent changes in usernames can be used as a tactic to obfuscate the user’s true identity.

25. On or about 28 June 2023, MANUELITO was arrested and taken into custody, subsequent to federal indictment number 5: 23-CR-200-M-RJ.

26. On or about 7 July 2023, SA Rodriguez was notified by MANUELITO’S military unit that in accordance with Army policy, they conducted a full inventory of his barracks room in preparation to transfer them to his family. Upon inventory, they noted several items in his barracks room which were capable of internet connection. These items included, but were not limited to, three cellular phones, an apple watch with cellular capability, a Wi-Fi router, and an X Box game console. The unit paralegal JOHNNIE D. Luna informed SA Rodriguez the items would be provided to MANUELITO’S family the morning of 8 July 2023.

27. On or about 8 July 2023, SA Rodriguez coordinated with JOHNNIE who had key access to Barracks Room 201B, 4822 Gruber Road, Fort Liberty, NC 28310, which previously belonged to MANUELITO. Upon arrival JOHNNIE unlocked the door and SA Rodriguez noted the room had been inventoried. JOHNNIE stated during the inventory the unit placed the digital items on the kitchen counter. JOHNNIE related MANUELITO’S family arrived from Arizona and

would come to the same barracks room to remove the belongings around 1000, 8 July 2023. Under exigent circumstances due to the risk of the digital evidence being destroyed, SA Rodriguez seized three cellular phones, and a 32GB SD card. SA Rodriguez conducted no additional searches.

28. For the reasons listed above, I assert that there is probable cause to believe the digital devices associated with MANUELITO were used in connection with the violation of 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) (receipt of CSAM, and attempt) and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of, or access with intent to view, CSAM, and attempt).. Based on my training and experience, a search of cellular telephones and removable media can contain stored images, videos, electronic communications, information concerning social media accounts, account access information, IP addresses, log files, and other relevant information. Therefore, the information described in Attachment B will constitute evidence of the aforementioned violations.

BACKGROUND CONCERNING MOBILE DEVICES

29. Based on my training and experience, I use the following technical terms to convey information in relation to cellular telephones:

30. Cellular telephone: A wireless telephone (or mobile telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing contact information such as names and phone

numbers in “address books” or contact information. Such devices are generally capable of sending, receiving, and storing text based messages to include iMessages, Short Message Service, Multimedia Messaging Service texts, and e-mails. Records and data associated with third-party applications may also be stored on devices; for example, Signal an instant messaging service. The devices are generally capable of creating, receiving, transmitting, and storing photographs, videos, and audio files including voicemails. Further they are generally capable of storing logs of dates, times, calendar information, notifications, and accessing and downloading information from the Internet. Cellular telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

31. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains historical location records for the device has been. GPS information is retrieved from satellites orbiting the Earth. These satellites transmit data via radio signals. When a GPS antenna receives signals it established the latitude, longitude, and sometimes altitude of the device. Some cellular devices insert GPS data into images and video files, which can aid in identification of victims of CSAM.

32. The stored communications and files maintained on the cellular telephone may provide direct evidence of the offenses under investigation. Based on my training and experience, social media chat logs, instant messages, emails, voicemails, photographs, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

33. In addition, activity logs, stored electronic communications, and other data retained by a cellular telephone can indicate who used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who utilized the cellular device at a relevant time.

34. Cellular telephones are capable of accessing the internet is a worldwide network that connects digital devices and allows communications and the transfer of data and information across state and national boundaries. A user can access the Internet from an Internet Service Provider (“ISP”) that connects to the Internet. The ISP assigns each user an Internet Protocol (“IP”) Address. Each IP address is unique. Every computer or device on the Internet is referenced by a unique IP address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 255. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the device from which those individual initiates access is assigned an IP address.

35. Those who sexually exploit children can transfer photographs and videos via the internet but must connect to an ISP whether it be through their carrier’s mobile data or a Wi-Fi connection. Once connected they will have an associated IP address. Electronic contact can be made to literally millions of computers and cellular phones around the world. The ability to produce CSAM easily, reproduce it inexpensively, and distribute it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of CSAM. Due to the proliferation of commercial services that provide electronic mail service, chat

services (i.e., "Instant Messaging"), and easy access to the Internet, digital devices are the most widely used method of distribution and receipt of CSAM.

36. In my training and experience, individuals who pursue CSAM use a variety of devices to obtain, view, distribute, and store the material. This often includes the use of removable storage devices, hidden or obfuscated electronics and the information contained within. As such removable media and cellular telephones often contain evidence and instrumentalities associated with the crimes under investigation.

CONCLUSION


37. Based on the forgoing, I request that the Court issue the proposed search warrant. I respectfully submit that there is probable cause for a search warrant authorizing the search and seizure of one TCL brand phone, IMEI: 01569500861147, one TCL brand phone, IMEI: 016144002543799, one Samsung brand phone, IMEI: 350593473858405, and one San Disk brand, 32GB thumb drive.

38. I respectfully request that the Court issue a warrant authorizing members of CID or their authorized representatives, including but not limited to other law enforcement agents and laboratory personnel assisting in the investigation, to obtain and analyze the devices.

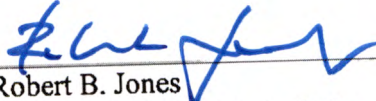
[Remainder of page intentionally left blank]

39. I request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. §§ 2251(A) (production of Child Sexual Abuse Material (CSAM)), 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) (receipt of CSAM, and attempt) and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of, or access with intent to view, CSAM, and attempt), and Federal Rule of Criminal Procedure 41.

Respectfully submitted,


Erika Rodriguez
Special Agent
US Army Criminal Investigation Division

Pursuant to Rule 4.1 of the Federal Rules of Criminal Procedure, the affiant appeared before me via reliable electronic means, was placed under oath, and attested to the contents of this affidavit this 13 day of July 2023.


Robert B. Jones
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

The devices include one TCL brand phone, IMEI: 01569500861147, one TCL brand phone, IMEI: 016144002543799, one Samsung brand phone, IMEI: 350593473858405, and one San Disk brand, 32GB thumb drive. Described as DEVICES in attachment B.

ATTACHMENT B

Particular Things to be Seized

I. Information to be seized by the government

1. All records on the devices, listed on Attachment A, that constitutes evidence of a violation of 18 U.S.C. §§ 2251(A) (production of Child Sexual Abuse Material (CSAM)), 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) (receipt of CSAM, and attempt) and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of, or access with intent to view, CSAM, and attempt), and information pertaining to the following matters:

- a. evidence of who used, owned, or controlled the DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. records of or information about Internet Protocol addresses used by the DEVICE.
- c. records of or information about the DEVICE’S Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses revealing an interest in child exploitation content.
- d. Child pornography, as defined in 18 U.S.C. § 2256(8).
- e. Records, information, and items relating to violations of the statutes described above in the form of:

- i. Records and information referencing child pornography, as defined in 18 U.S.C. 2256(8);
 - ii. Records and information referencing child erotica;
 - iii. Any and all information associated with applications downloaded to the DEVICES that references or reveals an interest in or the sexual exploitation of children.
- f. Evidence indicating the DEVICE user's knowledge and/or intent as it relates to the crime(s) under investigation, such as research into child exploitation statutes including;
 - i. Records and information referencing or revealing the sexual exploitation of children;
 - ii. Records and information revealing sexual interest in minors;
 - iii. Records and information referencing or revealing trafficking, advertising, or possession of child pornography;
 - iv. Records and information referencing or revealing communication or interaction of an illicit sexual nature with minors;
 - v. Records and information constituting or revealing membership or participation in groups or services that provide or make accessible child pornography; and

- vi. Records and information revealing the use and identification of remote computing services such as email accounts or cloud storage.
- g. Incoming and outgoing communications, including but not limited to calls, SMS messages, MMS messages, and any third-party application communications referencing or revealing an interest in or the sexual exploitation of children.
- h. Photos, Videos, or other images taken or saved to the DEVICES, or audio recordings, including any voice messages or voicemails, referencing or revealing an interest in or the sexual exploitation of children.
- i. Any records or notes, including names and telephone numbers of persons from whom it is suspected visual depictions of the sexual exploitation of children were traded;
- j. Records and information referencing or revealing access to and/or the use of Instagram, Kik Messenger, Cash App, and other social media and payment applications,
- k. Evidence of the attachment to the DEVICES of other storage devices or similar containers for electronic evidence;
- l. Passwords, encryption keys, and other access devices that may be necessary to access the DEVICES;

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits,

and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, CID may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.